REMARKS

The Non-Final Office Action mailed June 8, 2009 considered claims 1-32 and 53. Claims 1-32 and 53 were rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 1-32 were rejected under 35 U.S.C. 101 because the claimed invention was directed to non-statutory subject matter. Claims 1-29 and 53 were rejected under 35 U.S.C. 102(e) as being anticipated by Traw et al. (US 6,542,610) hereinafter *Traw*. Claims 30-32 were rejected under 35 U.S.C. 103(a) as being unpatentable over *Traw*.

By this amendment, claims 1, 3-5, 7-10, 12, 15, 17, 18, 20-29, 31, 32, and 53 are amended and claim 53 is new.[1] Accordingly, claims 1, 3-5, 7-10, 12, 15, 17, 18, 20-32, 53, and 55 are pending, of which claims 1, 53, and 55 are in the independent claims.

Applicants respectfully submit that the cited art of record does not anticipate or otherwise render the amended claims unpatentable for at least the reason that the cited art does not disclose, suggest, or enable each and every element of these claims

Traw describes content protection for digital transmission systems. *Traw* uses a preliminary authentication followed by a full authentication. (Col. 4, ll. 44-46). The preliminary authentication (or first level of security) permits compliant, but computationally constrained, devices (e.g., consumer electronic devices), to begin delivering content with low latency. (Col. 3, ll. 20-30 and ll. 3-31, Col. 4, ll. 14-24, Col 5, ll. 37-46, and Fig. 2). The preliminary authentication phase is designed to provide reasonable security for protected content while being computationally lightweight in order to maintain user transparency. (Col. 6, ll. 56-61). From preliminary authentication, preliminary control and content channels are established. Protected content can be then be transferred (with some level of security) while a more secure channel is established in the background (e.g., using full authentication). (Col. 4, ll. 18-26).

In some embodiments of *Traw*, a determination is made to whether a content source or sink is computationally constrained. If neither device is computationally constrained,

[1] Support for the amendments to the claims is found throughout the specification and previously presented claims of U.S. Pat. Publ. No. 2007/0234272, including but not limited to paragraphs [0027]-[0032], [0036], [0039], [0040], [0049]-[0052], [0065]-[0070], [0075]-[0078], [0081], and [0082] and Figures 1, 3, 5, and 7.

establishing preliminary control and content channels is bypassed. (Col. 4, ll. 28-33, Col. 6, l. 62 – Col 7, l. 5, and Fig. 1(b)).

During preliminary authentication, each device generates an expected value the other device expects to receive. Each device generates a text string from concatenating a random challenge and a device certificate. Each device transmits its generated text string to the other device. Each device encrypts the received random challenge (e.g., using the baseline cipher) and the hashes the encryption results to a form another data string. Each device then transmitted the other data string back to the other device. Each device compares the other string to an expected value (based on the original random challenge). If both values match, a preliminary control channel is generated. (Col. 7, ll. 16-41 and Fig. 3(a)). Compliant systems must implement required components for sourcing and receiving content. (Col 10, ll. 52-58, Figs 6 and 7).

From a match, a device essentially infers that the other device has the appropriate functionality of the required components to protect content. However, since the values are derived from random challenges, the values themselves do not expressly prove that the other device includes required components. Thus, *Traw* fails to teach or suggest (as recited in claims 1 and 53):

- an act of the computer system accessing information that indicates how to prove an appropriate configuration, from among one or more appropriate configurations, to access the resource in accordance with the one or more security policies subsequent to and in response to successfully conducting application authentication, *the accessed information indicating that one or more application measurable aspects of the distributed application component and one or more computer system measurable aspects of the computer system are to be verified to prove that the combination of the distributed application component and the computer system provide an appropriate configuration to interoperate with the other distributed application component to access the resource*
- an act of the processor formulating an assertion that can used to verify the one or more application measurable aspects and the one or more computer system measurable aspects, *the assertion representing identity values for the one or more application measureable aspects and representing environment values for the one or more computer system measurable aspects, the identity values expressly indicating the identity and the functionality of portions of computer-executable instructions included the distributed application component, the environment values identifying the execution environment at the computer system*

Accordingly, the cited art fails to teach or suggest either singly or in combination:

...

an act of the computer system accessing information that indicates how to prove an appropriate configuration, from among one or more appropriate configurations, to access the resource in accordance with the one or more security policies subsequent to and in response to successfully conducting application authentication, the accessed information indicating that one or more application measurable aspects of the distributed application component and one or more computer system measurable aspects of the computer system are to be verified to prove that the combination of the distributed application component and the computer system provide an appropriate configuration to interoperate with the other distributed application component to access the resource;

an act of the processor formulating an assertion that can used to verify the one or more application measurable aspects and the one or more computer system measurable aspects, the assertion representing identity values for the one or more application measureable aspects and representing environment values for the one or more computer system measurable aspects, the identity values expressly indicating the identity and the functionality of portions of computer-executable instructions included the distributed application component, the environment values identifying the execution environment at the computer system; and

...

as recited in claims 1 and 53, when view in combination with the other limitations of claims 1 and 53. For at least this reason, claims 1 and 53 patentably define over the art of record. Since each of the dependent claims depends from claim 1, any dependent claims patentably define over the art of record at least for the same reason as claim 1. However, many of the dependent claims also independently distinguish over the art of record.

For example, the cited art fails to teach or suggest either singly or in combination, "accessing a request for byte values included in the computer-executable instructions of a specified version of the distributed application", as recited in claim 10. For at least this further reason, claim 10 patentably defines over the art of record. Further, the cited art fails to teach or suggest either singly or in combination an "assertion is formulated proof that can be used to

verify byte values included in the computer-executable instructions of a specified version of the distributed application", as recited in claim 12. For at least this further reason, claim 12 patentably defines over the art of record. Additionally, the cited art fails to teach or suggest either singly or in combination "digitally signing bytes taken from one or more identified code regions of computer-executable instructions within the distributed application", as recited in claim 29. For at least this further reason, claim 29 patentably defines over the art of record.

The cited art also fails to teach or suggest either singly or in combination:

...

an authentication module configured to:

conduct machine authentication with other computer systems, including establishing a Secure Sockets Layer (SSL) connection between the computer system and the other computer systems;

wherein the application authentication module is configured to:

conduct application authentication with distributed application components of the distributed application at other computer systems after the other computer systems have been authenticated using machine authentication so that the computer system can verify the identity of the other distributed application component, application authentication including the computer system receiving proof from the other distributed application components that the other distributed application components comply with one or more security policies of the computer system; and

wherein the distributed application component is configured to:

access information that indicates how to prove an appropriate configuration, from among one or more appropriate configurations, to access the resource in accordance with the one or more security policies subsequent to and in response to successfully conducting application authentication, the accessed information indicating that one or more application measurable aspects of the distributed application component, including access to specified byte values from within specified locations in computer-executable instructions of the distributed application, and one or more computer system measurable aspects of the computer system, including specified values for specified execution environment

variables, are to be verified to prove that the combination of the distributed application component and the computer system provide an appropriate execution environment for interoperating with the other distributed application component to access the resource;

formulate an assertion that can used to verify the one or more application measurable aspects and the one or more computer system measurable aspects, the assertion including the specified byte values from within the specified locations in computer-executable and the specified values for the specified execution environment variables

as recited in claim 55, when viewed in combination with the other limitations of claim 55. For at least this reason, claim 55 also patentably defines over the art of record.

Claims 1-32 and 53 were rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. As per claims 1 and 53 it is uncertain who is "accessing" an indication and where the "indication" comes from. By this amendment, claims 1 and 53 are amended to better define the components perform the language recited in claims. Applicants submit that the amended claim language overcomes the 35 U.S.C 112, second paragraph, rejections. Accordingly, Applicants respectfully request that the rejections of claims 1-32 and 53 under 35 U.S.C 112, second paragraph, be withdrawn.

Claims 1-32 were rejected under 35 U.S.C. 101 because the claimed invention was directed to non-statutory subject matter. By the amendment, claim 1 is amended to recite "an act of the processor formulating an assertion that...". Applicants submit that amended claim language ties the limitations of claim 1 to a hardware device for implementing the recited claim language. Applicants submit that the amended claim language overcomes the 35 U.S.C 101 rejections. Accordingly, Applicants respectfully request that the rejections of claims 1-32 under 35 U.S.C 101 be withdrawn.

In view of the foregoing, Applicants respectfully submit that the other rejections to the claims are now moot and do not, therefore, need to be addressed individually at this time. It will be appreciated, however, that this should not be construed as Applicant acquiescing to any of the purported teachings or assertions made in the last action regarding the cited art or the pending application, including any official notice. Instead, Applicant reserves the right to challenge any

of the purported teachings or assertions made in the last action at any appropriate time in the future, should the need arise. Furthermore, to the extent that the Examiner has relied on any Official Notice, explicitly or implicitly, Applicant specifically requests that the Examiner provide references supporting the teachings officially noticed, as well as the required reason why one of ordinary skill in the art would have modified the cited references in the manner officially noticed.[2]

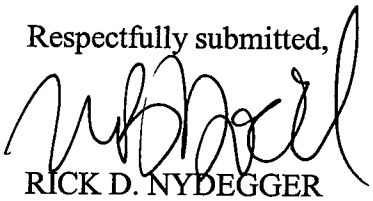
In the event that the Examiner finds remaining impediment to a prompt allowance of this application that may be clarified through a telephone interview, the Examiner is requested to contact the undersigned attorney at (801) 533-9800.

[2] Instead, Applicant reserves the right to challenge any of the purported teachings or assertions made in the last action at any appropriate time in the future, should the need arise. Furthermore, to the extent that the Examiner has relied on any Official Notice, explicitly or implicitly, Applicant specifically requests that the Examiner provide references supporting any official notice taken. Furthermore, although the prior art status of the cited art is not being challenged at this time, Applicant reserves the right to challenge the prior art status of the cited art at any appropriate time, should it arise. Accordingly, any arguments and amendments made herein should not be construed as acquiescing to any prior art status of the cited art.

The Commissioner is hereby authorized to charge payment of any of the following fees that may be applicable to this communication, or credit any overpayment, to Deposit Account No. 23-3178: (1) any filing fees required under 37 CFR § 1.16; and/or (2) any patent application and reexamination processing fees under 37 CFR § 1.17; and/or (3) any post issuance fees under 37 CFR § 1.20. In addition, if any additional extension of time is required, which has not otherwise been requested, please consider this a petition therefore and charge any additional fees that may be required to Deposit Account No. 23-3178.

Dated this 11th day of August, 2009.

Respectfully submitted,



RICK D. NYDEGGER
Registration No. 28,651
MICHAEL B. DODD
Registration No. 46,437
Attorneys for Applicant
Customer No. 47973

RDN:jml:crb
2454609_1